Technology, Intelligence, and TRUST

Troops receive intelligence briefing before Mosul raid

U.S. Air Force (Vanessa Valentine)

By JAMES R. HOWCROFT

The outcome of the conflicts that the American military is likely to fight in the decades ahead will increasingly depend on tactical success and the empowerment of small unit leaders. Recent advances in technology have the potential to improve the intelligence collection and dissemination capabilities of tactical military units. Unfortunately, perceptions about who "does" intelligence and the role and responsibilities of intelligence collection, analysis, and dissemination threaten to limit the warfighting potential of intelligence technology on the battlefields of the 21st century. A mindset change is required to maximize the evolving capabilities of modern technology.

Cold War Intelligence Paradigm

During the Cold War, much of our intelligence collection was centralized at the national level and focused on strategic targets, which were seen as the key to victory against conventional armed forces. Cold War targets were generally static sites, such as headquarters, missile silos, airfields, or railroad marshalling yards. Intelligence collection was prioritized to provide accurate targeting data and follow-on bomb damage assessment on these targets for manned and unmanned airborne weapons platforms. The requirements of ground-based tactical and operational level intelligence consumers were only of secondary importance; units at this level were not critical to success. Victory was won or lost at the strategic level.

Strategic level headquarters naturally determined the target sets for this Cold War intelligence collection. Units at the operational or tactical commands could input collection requests, but these requests required validation by every headquarters in the command hierarchy prior to arrival at the national tasking level. The requirements of a unit lower in the hierarchy could be trumped by anyone higher in the chain. In this process, tactical units had little or no visibility. Transparency did not exist to allow a tactical consumer to determine easily when or if his requirement would be collected.

Ironically, the tactical commander who had the most pressing need for the greatest resolution of the battlefield had the least ability to access or influence the centralized intelligence collections architecture. In 2003, following the invasion of Iraq and the capture of Baghdad and Tikrit, the 1st Marine Division in its official after-action report noted, "The Byzantine collections process inhibited our ability to get timely responses to combat requirements. . . . The existing hierarchical collections architecture is wildly impractical and does not lend itself to providing timely support to combat operations."[1]

Sadly, much of this Byzantine bureaucracy is with us still today. In addition to the burden of competing with every unit above him in the collections chain, the tactical consumer must depend on a collections hierarchy to push critical intelligence down to him rapidly in an accessible, relevant format. The tactical consumer is dependent on those above him in the distant headquarters who carried out the collection and analysis of the raw data to understand and appreciate his

Colonel James R. Howcroft, USMC, serves as the U.S. Marine Corps Chair and Military Professor of International Security Studies at the George C. Marshall Center for European Security Studies in Garmisch-Partenkirchen, Germany. He is a career Intelligence Officer.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **2007**	2. REPORT TYPE	3. DATES COVERED **00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE
Technology, Intelligence, and TRUST

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
National Defense University,Institute for National Strategic Studies,260 Fifth Ave SW (BG 64) Fort Lesley J McNair,Washington,DC,20319

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**7**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

specific information needs. If the tactical consumer were successful at precisely describing his requirements days ahead of time and in a manner and method that were understandable to the analyst conducting the "readout" of the collection data, he might just be fortunate enough to receive a useful product.

While Service-centric intelligence is a step in the right direction, the military consumer is still U.S. Central Command or U.S. European Command headquarters in Tampa or Stuttgart, respectively (at least in the eyes of the distant national level intelligence agencies), not an infantry battalion on the Syrian border. The distant analyst often has little visibility or understanding of exactly why the tactical consumer is asking for the information, the impact of the data, or how to package the information so it is actionable for the ground commander.

For example, if the tactical consumer in his formalized collections request asks for information regarding the presence of armored vehicles at a given set of coordinates, the analyst looks for and reports on that particular informational request at that specific place—not on the implied request for trafficability, presence of an artillery battery 10 kilometers away, or the presence or absence of a bridge or tactical fortifications. The communications connectivity and permissions rarely exist for a direct and timely dialogue between the tactical consumer and the distant analyst to define and refine the evolving needs of the consumer.

Once in combat, the needs of tactical intelligence consumers are time-sensitive and can rarely be supported by a hierarchy dependent on the flow and validation of information and permission up the chain of command and then back down this same chain once the intelligence has been collected and analyzed. This is not to say that national level collection is never responsive to tactical consumers, but information passed down to the consumer in a timely manner is still a rarity that requires an almost serendipitous convergence of adequate time, an analyst at the collections level who precisely understands the stated and implied requirements of the tactical user, no interference by higher headquarters to trump the tactical request, and adequate communications means.[2]

the tactical commander who had the most pressing need for the greatest resolution of the battlefield had the least ability to access or influence the centralized intelligence collections architecture

In the past, tactical units were perceived—and perceived themselves—primarily as consumers of intelligence, not producers. Intelligence in this hierarchical model was seen as a commodity produced at higher headquarters (HHQ), which controlled the assets, validated and prioritized the intelligence requirements, and was then responsible for disseminating down the hierarchical chain the intelligence that it determined tactical units needed. During my career as an intelligence officer, I was told on numerous occasions, "Trust us, when the balloon goes up, you'll get all the intelligence you need." Intelligence was something that one went to HHQ to receive. Since HHQ owned and controlled intelligence, the (natural) perception within the hierarchy was that HHQ had the most accurate picture of the chaotic battlefield. This has led to a mistaken and misdirected concept that a relevant and accurate intelligence "common operating picture" can be produced at a senior headquarters and pushed down to a tactical unit.

Soldiers gather intelligence during Baghdad raid

U.S. Army (Tierney Nowland)

Evolving 21st Century Requirements

The dynamics of the current battlefield have changed the intelligence paradigm. This is true regardless of whether the foe is a conventional or an asymmetrical threat. While few conventional foes exist to challenge the American military now, those that do exist are defeated not by attrition but by our attacking their cohesion as a military entity. While part of this effort to destroy enemy cohesion entails attacking "traditional" fixed targets, such as headquarters buildings, airfields, or logistics nodes, speed at the tactical and operational levels is increasingly a weapon to be wielded against conventional or asymmetric foes. Success depends on the tactical commander quickly recognizing and immediately exploiting fleeting opportunities as they present themselves on the battlefield. These opportunities are most often visible only to engaged commanders, not to distant HHQs far removed from the battlefield.

This high operational tempo requires, indeed demands, informed decisionmaking on the spot by lower level units. The present hierarchical collection and dissemination chain is too slow and cumbersome to provide intelligence that is relevant and actionable to the tactical commander. While it is possible to reach back for information (intelligence pull) or for this information to be pushed down the hierarchical chain of command (intelligence push), intelligence must be "personalized" to be relevant for the battlespace of each commander. Even military units in the early stages of defense transformation engaged in battle against symmetrical foes have outgrown the archaic system's capability to provide them with relevant, actionable intelligence on the battlefield. In March 2003, for example, once the 1st Marine Division crossed the Iraq-Kuwait border, "the Division received very little actionable intelligence from external intelligence agencies."[3] National level collection and dissemination systems were unable to keep pace with the dynamic environment—even against a symmetrical conventional foe. The national level system was hard at work but lacked an appreciation for the tactical situation on the ground and could not convert collected information into actionable intelligence.

success depends on the tactical commander recognizing and immediately exploiting fleeting opportunities

While the conventional military forces of foes such as China and North Korea still pose an ominous threat, the more likely scenarios for military employment are in counterinsurgency and stabilization operations. The 2006 Quadrennial Defense Review Report notes that "irregular warfare has emerged as the dominant form of warfare confronting the United States" and directs that future warriors "be as proficient in irregular operations, including counterinsurgency and stabilization operations, as they are in high intensity combat."[4] More so than the conventional wars of the past, counterinsurgencies and stabilization operations are fought at the tactical level. Tactical success may not equate to strategic victory; indeed, tools wielded by other agencies and departments are now often of greater importance in achieving strategic success, however defined.

What is clear is that strategic success is not the result of the destruction or capture of a single objective or individual. Capturing and killing Saddam, killing his sons, or killing Abu Musab al-Zarqawi have not led to victory in Iraq. Capturing or killing Osama bin Laden will not end the war on terror or result in victory in Afghanistan. Shock and awe do not apply. The target set is not there. As seen in Afghanistan in 2001, the ability to destroy headquarters or bridges or crater airfields is irrelevant in fighting the asymmetrical foe. Destroying fixed nodes is not only irrelevant; it also is counterproductive during counterinsurgency or stabilization operations.

Marine configures Trojan Lite satellite communications system

An important factor to consider when weighing current intelligence requirements is the fact that Soldiers will increasingly be deployed within growing urban sprawl. The current ability to collect intelligence using strategic assets in this environment is limited. While it may be possible to image individual buildings with great resolution, we still cannot see who is inside, whether he is armed, or if he is hostile. It requires a man on the ground to go into the building or to communicate face-to-face with the inhabitants of the neighborhood to collect and evaluate the intelligence. Even if it were possible with technology to determine that certain individuals within an individual building were hostile,

U.S. Marine Corps

striking urban targets with strategically controlled weapons carries with it the likelihood of civilian destruction and death.

If the point of the main effort is increasingly likely to be at the tactical level, then the intelligence focus also needs to shift to reflect this evolved paradigm. A shift in intelligence focus entails not only a reorientation in collection tools, intelligence manning, and analysis that is responsive to and supportive of the tactical commander, but also a deeper shift regarding intelligence responsibility and trust within the command hierarchy and the Intelligence Community.

Talking about intelligence in this new environment is impossible without first addressing communications. Intelligence and communications are inextricably linked. Technology is moving to fill the capability gap regarding high-bandwidth communications to dispersed tactical users. Advances in the ability of tactical units to be part of a wider information network hold great promise. Larger amounts of data can be moved faster, and tactical units have an enhanced capability to receive and send information via the communications network. Fortunately, the headquarters of tactical units are generally static during counterinsurgency and stability operations, which allows them access to the common communications network that they would lack if on the move in a conventional fight. Networked systems have the potential to allow widely scattered units within the hierarchy to have simultaneous access to intelligence. With the proper permissions, tactical, operational, and strategic consumers can pull required information from throughout the network and tailor the product to meet their own specific intelligence needs.

Decentralized Focus and Tools

Tactical commanders require decentralized collection tools that respond immediately to their needs. The belief that a few capable centralized national systems alone are able to meet the needs of the tactical consumer is flawed. Regardless of the technological capability of the collection platform, a tactical commander must still battle the collection validation bureaucracy and can still be trumped by anyone in his chain of command. The tactical commander needs his own intelligence collection toolkit to complement the national systems. This toolkit could include small-scale unmanned aircraft systems and unmanned ground vehicles that are simple and rugged enough to be operated by Soldiers and Marines, not contractors.

networked systems have the potential to allow widely scattered units within the hierarchy to have simultaneous access to intelligence

The Dragon Eye system, for instance, launched by a bungee cord and controlled via a laptop computer by a single Marine with an afternoon of training, is an example of a tactical collection tool with limited range, but one that is still responsive and can see over the next hill to provide “eyes-on” intelligence. Small seismic intrusion detectors, backpack ground surveillance radars, miniature motion sensors, and remote video cameras are examples of the technology that exists today that must be placed in the hands of tactical commanders to help prevent tactical surprise. While technology of this type is valuable, it is important not to lose sight of the fact that the ultimate collection tool is a culturally attuned, language-capable Soldier or Marine who appreciates the context of the tactical environment in which he employs these tools. The investment should be in tactical systems to support this collector—not on national systems, more data infrastructure, or more buildings manned by analysts located far from the fight.

Similarly, intelligence collection teams attached to tactical units need to understand the requirement to provide immediate support to the tactical commander. Fortunately, human intelligence and signals intelligence collections teams operating in a tactical commander's battlespace now accept that their primary and immediate focus of collection and dissemination should be the local unit. It is unacceptable for reporting and the collection "take" to be passed up the chain of command and only be pushed back down to the tactical consumer after it has been analyzed and "massaged." By this time, the information has lost relevance or is so sanitized to protect its source that it has become worthless. The teams need to focus on time-sensitive, actionable intelligence to the tactical commander rather than on collecting information to be entered into a national level database. Fortunately, with contemporary networked communications, it is possible to have multiple addressees on a single email or message. The collections team does not have to make an either/or decision about whom to send its intercept or interrogation report to (either the battalion in whose battlespace the team is located or its higher headquarters). Now it can do both simultaneously.

additional tools, databases, and increased connectivity do not replace intelligence professionals at the tactical level

Similarly, an analyst at a facility removed from the tactical battlespace must have an appreciation of which time-sensitive information is relevant and actionable for the local commander. He must then be aware of which units are responsible for particular battlespaces so he knows specifically whom to include on his dissemination list when he transmits perishable intelligence. With the communications tools available today, pushing an intelligence product up the chain of command without immediate dissemination to the affected tactical unit is irresponsible. Unit boundaries and the hierarchical chain of command must not become barriers and impediments to time-sensitive support to those on the ground. Informal networks and peer cross-talk can serve to work around these artificial unit-based barriers, but peer cross-talk should supplement and refine regular reporting, not substitute for it.

This type of responsive, responsible collection and dissemination, which maximizes the capabilities of networked communications, depends on collectors being trusted by higher headquarters and granted the authority to disseminate their products directly to the tactical user as well as the wider community, without validation or "scrubbing" by a hier-

U.S. Marine Corps (Patrick Johnson-Campbell)

Marine collects short-range reconnaissance data

U.S. Marine Corps (Kenneth Madden)

Marines operate ground-control station for Dragon Eye unmanned aircraft system

archy seeking to ensure completeness or conformity with the assessments of a senior headquarters. When provided with a larger share of raw intelligence, the tactical consumer must be trusted not only to safeguard the specific capabilities of intelligence platforms (that is, sources and methods) but also to understand that raw intelligence data is often contradictory or wrong and may require corroboration before action. But it is, in fact, often the tactical commander, with an intimate knowledge of his battlespace and therefore the best understanding of the environment, who is best suited to corroborate and provide the proper context for the raw data.

Intelligence Manning Implications

If indeed the intelligence focus of effort is at the tactical level, then intelligence manning should reflect this fact. Tactical units currently lack adequate manning in their intelligence section to conduct a counterinsurgency campaign or to conduct stability operations for months at a time—24 hours a day, 7 days a week. A tactical commander equipped with his own organic collections tools will find his intelligence section quickly overwhelmed. Additional tools, databases, and increased connectivity do not replace intelligence professionals at the tactical level; on the contrary, they actually demand a personnel increase. Indications are that many tactical commanders in Iraq have dealt with this issue by shifting Soldiers and Marines from other table of organization billets into their intelligence sections.

The intelligence support teams provided to the tactical commander must be, as much as possible, attached early enough before deployment to give the supported unit and the intelligence attachments the time to develop a habitual relationship and build trust and confidence within the team. Commanders and staffs process information and intelligence in different ways and at different speeds. Prior to deploying, a commander must be able to see the capabilities of his organic and attached intelligence assets to understand their applicability and utility. He needs to know in advance just what their footprint is and what support requirements they entail. Prior to the invasion of Iraq in 2003, Trojan SPIRIT LITE communications systems and remote receive stations for unmanned aircraft systems were attached to several regiments in the 1st Marine Division. While planning and coordination were done ahead of time, transportation and logistics issues delayed their attachment with the regiments until the last minute. Predictably, the results were disappointing. In some cases, the regiments, faced with competing time and attention requirements, never had the chance to work through the difficulties involved in assimilating unfamiliar new systems and people. It is important to build cohesion, trust, and communication prior to the stress and rigor and fatigue of combat. Once attached, every attempt should be made to keep the tactical intelligence team together, rather than "robbing Peter to pay Paul" in response to emerging requirements or a perceived crisis elsewhere.

Responsibility and Trust

This shift to an increased tactical focus entails a transformation in the concept of intelligence responsibility and trust on the battlefield. No longer do senior headquarters have the most accurate view of the critical battlefield. The tactical commander, immersed 24/7 in the cultural nuances of his local environment, is now, more than ever, in possession of the most accurate picture of the battlefield. It may be only a small piece, but just as operational success is an accumulation of tactical successes, so is an accurate intelligence picture at the operational level an accumulation of smaller, accurate intelligence pictures from below. Having this information entails a responsibility for tactical commanders, armed with additional collections tools and analytical capability, to paint a relevant, precise picture for everyone else, including the other players and actors present on the contemporary battlefield. This reporting from the tactical level can then be used by analysts throughout the hierarchy to develop a tailored intelligence product for their respective commanders and staffs. The tactical commander now can, and must, send his reporting throughout the wider communications network.

senior commanders and their staffs need to step back from the tactical battle and focus on the war at their particular level

This paradigm entails a change in the trust relationship within the hierarchy. Previously, tactical commanders and intelligence officers relied on their higher headquarters to provide them needed intelligence. Now, HHQ must trust their subordinates to portray the battlefield. The immediate higher headquarters in the hierarchical chain has to trust its subordinate to input intelligence into the network that will be accessible and visible to all. If the raw intelligence reporting from the tactical commander has to be routed or cleared by HHQ prior to dissemination, the advantage is nullified. Higher headquarters, in turn, has to be trusted not to second guess and micromanage tactical commanders and must accept that lower level commanders know what is best within their zones. They must understand that their role is to assign the mission, provide commander's guidance, prioritize the required resources—and then step aside.

Empowerment is a term loosely thrown around. True empowerment is HHQ entrusting tactical commanders with authority and assets to assess the situation locally and do what needs to be done to accomplish the assigned mission. Once they have entrusted their subordinates, higher headquarters must resist the temptation to intervene. Communications and collection advances have made it possible for distant senior commanders and their staffs to monitor, in real time, the tactical or operational situation in their subordinate units. This ability to view is not necessarily the same as the ability to understand; the context is missing. Due to the hierarchical nature of the military, most commanders previously have held the job of their subordinates. This tendency, combined with the increased ability to monitor and communicate directly to subordinates throughout the chain of command, compounds micromanagement. Just because a senior headquarters has increased connectivity, it does not mean that exercising that capability is the right thing to do.

Senior commanders and their staffs need to step back from the tactical battle and focus on the war at their particular level, rather than interfering in their subordinates' domain. Subordinates have to be trusted to do what needs to be done within their battlespace to achieve the mission assigned by their HHQ. Despite talk of empowerment, interference and micromanagement are, unfortunately, increasingly the norm. An example of this micromanagement was the order in March 2003 to I Marine Expeditionary Force (I MEF), while it was attacking toward Baghdad, to divert a brigade from the point of main effort to deal with Iraqi divisions along the Iranian border on the MEF eastern flank. The Iraqi divisions had long been a focus of the I MEF, who had conducted an in-depth risk assessment, continually refined and updated this assessment, and concluded that the Iraqi divisions were adequately addressed by information operations, airstrikes, and persistent surveillance sufficient to provide early warning should the divisions decide to leave garrison. Distant commanders, viewing the battlefield without the context, directed the diversion of precious ground combat power to attack Iraqi divisions that were already out of the fight.[5]

As the ability to gather information has grown, staffs at military headquarters have grown to keep pace with the perceived need to manage the information. Subordinate headquarters are overwhelmed with the need to "feed the beast"—to satisfy the voracious need for information to fill in a box on a briefing slide for a staff officer's portion of his commander's daily update. Just as the subordinate must be empowered and trusted to portray the situation relevant to his battlespace, the subordinate must trust his senior headquarters to exercise discipline not to micromanage the ongoing fight or overwhelm the subordinate with requests for nonessential data. It is difficult to exercise this discipline. The concept of "need to know," as currently employed, is most often used by a senior headquarters to limit information or intelligence to a subordinate. Is it unreasonable for this concept to work both ways? Is it unreasonable for a subordinate to ask his higher headquarters what it would do differently if the subordinate provided HHQ the requested information?

It is difficult for well-intentioned senior officers merely to observe and not interfere. It is extremely difficult in our hierarchical military for a staff officer to tell his boss, "General, I decided our headquarters won't access the video feed from the unmanned aircraft system for today's raid; our need to monitor isn't as important as the requirement of the battalion conducting the operation. If everyone logs into the site to monitor the mission, it slows down video feed to the battalion conducting the raid."

In this first decade of the 21st century, we have seen advances in technology that have the potential to provide the military commander with an unparalleled ability to monitor and collect intelligence on the battlefield. The questions become how to use this technology and which technology to buy. Based on the wars we will probably fight and our contemporary doctrine, it seems clear that there is a need to develop a number of smaller, decentralized collection systems rather than depend on a few, more capable systems managed and directed by a distant centralized hierarchy. To be effective, this decentralized intelligence collection demands continued development of the communications network to tie together tactical, operational, and strategic reporters and consumers.

This decentralized technology must be combined with a mentality shift that stresses that intelligence is something that everyone does. Everyone is a collector, and intelligence is not something delivered from above. Hand in hand with technological advances, there needs to be a realization of the vital human factor involved in order to maximize the technological potential. This human factor is trust: it is the trust to empower a subordinate and depend on him to complete his mission and fulfill his intelligence collection and reporting requirements. It is the trust of a subordinate in his higher headquarters that he will be given the tools and latitude to accomplish his mission without interference, second-guessing, and endless data requests from his higher headquarters. Without the effort to develop and maintain this trust, modern militaries will fall short in maximizing their potential. **JFQ**

NOTES

[1] 1st Marine Division, "Operation Iraqi Freedom (OIF): Lessons Learned," May 29, 2003, available at <www.globalsecurity.org/military/library/report/2003/1mardiv_oif_lessons_learned.doc>.

[2] One such success was the ability of lead regiments within the 1st Marine Division, via attached Trojan SPIRIT LITE communications systems, to reach back to the National Geospatial-Intelligence Agency (then the National Imagery and Mapping Agency) Web site to access accurate and timely intelligence on Iraqi ground forces hours prior to attacking across the Iraq-Kuwait border to capture the Rumaliya oilfields and associated national oil infrastructure in March 2003.

[3] 1st Marine Division.

[4] *Quadrennial Defense Review Report* (Washington, DC: Department of Defense, February 6, 2006), 36.

[5] Personal experience and observation by the author. For additional detail of this episode, consult Michael R. Gordon and Bernard E. Trainor, *Cobra II: The Inside Story of the Invasion and Occupation of Iraq* (New York: Pantheon Books, 2006).